Journal of Research in Science and Engineering (JRSE)
ISSN: 1656-1996 Volume-8, Issue-2, February 2026
DOI: 10.53469/jrse.2026.08(02).01

Artificial Intelligence and Machine Learning Applications in Infrastructure Security

Navanithan Shanmugam

Abstract: ***The fintech sector is one of the ideal targets for cybercriminals. Due to the sector's reliance on online platforms and the financial viability of fintech companies, attackers find fintech companies favorite targets. To mitigate the rising cybersecurity threat in the sector, fintech companies are increasingly incorporating artificial intelligence and machine learning models in their infrastructure security. This writing discusses the increasing cybersecurity threat in the fintech sector and explores how AI and ML are being leveraged in fintech cyber security.***

Keywords: fintech sector, cybercriminals, online platforms, financial viability, cybersecurity threat, artificial intelligence, machine learning, infrastructure security

1. Introduction

With the proliferation of technology in the financial industry, the fintech sector has emerged as one of the fastest-growing segments in the finance industry. According to Vantage Market Research (2023), the fintech sector was valued at $133 billion in 2022 and is projected to be valued at $556 billion in 2030, denoting a compound annual growth rate (CAGR) of 19.5 percent over the period. The growth of fintechs is being powered by the growing need for e-commerce services and mobile banking platforms that offer user-friendly environments for executing transactions.

Although the fintech sector offers a myriad of benefits for businesses and end users, this convenience comes at a price. Since the advent of fintech solutions, the sector has been subject to cybersecurity threats that have not only caused financial harm to businesses and consumers but also resulted in the loss of users' data. Although various mitigation mechanisms, such as encryption methods, firewalls, and multi-factor authentication, have been explored to address the rising cybersecurity threat on fintechs, the attacks have remained incessant and seem to be worsening.

Cybersecurity threat in fintechs

The financial sector is among the favorite targets for cybercriminals. Institutions in this sector handle large amounts of financial data, making them ideal targets for online fraudsters. Besides handling financial data, fintechs operate within wide networks to reach more users. While broad networks enable these institutions to reach more customers, they increase the attack surface for cybercriminals, making them easy targets. It is also worth noting that fintech firms tend to have the financial power to pay ransom, making them valuable targets for cyberattacks (Adeyoju, 2019). According to Fintech Magazine (2022), in 2020, 47 percent of Americans experienced financial identity theft, which has been growing by 40 percent annually.

Attacks directed at fintech companies include ransom, payment card theft, and illicit transfers. Ransomware attacks involve hackers accessing fintech systems and deploying encryption tools that encrypt system data and only decrypt it after extorting victims. Payment card theft entails attackers stealing customers' credit card information and using the credentials for illegal purchases. Payment card theft is among the most common attacks targeted toward fintechs and established financial institutions such as Equifax and JP Morgan Chase. Illicit transfers constitute aspects of account takeover. These types of attacks entail hackers accessing users' accounts and transferring money. According to Consumer Affairs, identity theft and illicit transfer cases have risen by over 584 percent over the past decade.

The consequences of cyberattacks on fintechs are dire. Besides financial losses, fintechs affected by cyberattacks face lawsuits, which sometimes result in their operational licenses being suspended. With the advent of cybersecurity laws such as the European Union's General Data Privacy Regulation (GDPR), fintechs that suffer data breaches may be subject to penalties (Najaf et al., 2021). Besides financial and legal ramifications, cyberattacks subject fintech organizations to reputational implications. High-impact digital breaches erode consumer trust, prompting them to migrate to competitor service providers. Due to the implications of cyberattacks on fintechs, it is vital for businesses to invest in novel technologies to curb the threat. Use of AI and machine learning is one of the emerging trends in the cybersecurity field that has shown the potential to bolster cyber systems security.

AI and machine learning in fintech cybersecurity

Artificial intelligence and machine learning are emerging technologies conventionally leveraged in marketing and sales. However, recently, the applications of these technologies have subtly begun finding their way into the cybersecurity sector. Although cybersecurity still heavily relies on human input, ultramodern cybersecurity frameworks are increasingly exploiting AI and ML models to detect, prevent, and thwart cybersecurity threats (Kamoun et al., 2020). Contemporary fintechs are employing these technologies to address human weaknesses that allow attacks. Some of the human weaknesses AI and ML are mitigating to prevent attacks include;

Configuration errors: Human errors are significant contributors to cybersecurity risk. Modern cybersecurity systems are complex, with many configurations. Configuring these systems can be challenging, even for organizations with large IT teams. AI and ML technology

can automate some configurations, reducing the workload of IT teams and enhancing configuration accuracy.

Human inefficiency with repetitive tasks: A majority of cybersecurity tasks are repetitive. For example, system configurations must be conducted after every update or event in the system. Repetitive tasks can become monotonous and boring. AI and ML technologies can be used to automate repetitive tasks, allowing human resources to focus on more productive tasks.

Threat alert fatigue: The attack surfaces are growing as fintech organizations deploy more elaborate and sprawling systems to serve increasing customers. Human teams are finding it laborious to monitor complex systems 24/7. Machine learning and artificial intelligence technologies can autonomously monitor sophisticated systems and generate alerts in real-time 24/7.

Threat response time: Threat response time is a significant factor in minimizing the damage caused by cyberattacks. Human teams can be overwhelmed by the speed of attacks, limiting their ability to respond promptly. Automated systems have proven to be effective in responding to attacks.

Threat prediction: New threats are emerging continually, making it difficult for cybersecurity experts to anticipate them. According to the Fugue report (2020), 84 percent of IT teams acknowledge being concerned about their systems being attacked without their knowledge. AI and ML-enabled systems have data analytics capabilities. This ability allows them to predict both known and unknown threats.

Applications of AI and ML in fintech infrastructures
The applications of AI and ML in fintechs' cybersecurity systems are diverse. Fintechs' cybersecurity systems can employ AI and ML models to detect and respond to cyber threats in real-time. As aforementioned, these technologies can analyze vast amounts of data to detect anomalies and predict impending risks. Some of the applications of machine learning and artificial intelligence in Fintechs' security systems include;

Fraud detection: Most frauds are perpetrated as phishing attacks in the fintech sector. According to insights from Mission Critical Magazine (2022), in 2022, phishing attacks on fintechs were 2.5 times more than in the previous two years. Deployment of AI and ML technologies in fintech promises to combat the rising fraud risk. Using historical data, AI and ML models can accurately detect fraudulent transactions and stop them in real-time. PayPal is one of the most popular fintech apps leveraging AI and ML models to detect and prevent fraudulent transactions such as money laundering and account takeovers.

Data security: Fintechs' business operations are powered by data. To provide personalized digital services, fintech services must collect, store, and process customer data to retrieve actionable insights such as customer tastes and preferences. ML and AI technologies can be leveraged to protect data breaches. These models can recognize attack patterns and flag suspicious operations on databases.

Vulnerability management: ML and AI models can help mitigate threats by conducting common vulnerabilities and exposures (CVE) data and proposing strategies for safeguarding fintech systems.

Threat intelligence: Threat intelligence is integral in combating known and unknown cyber threats. AI and ML algorithms deployed in fintechs' infrastructures can analyze data from varied digital sources such as commercial threat feeds, social media platforms, dark web, and open-source threat intelligence, and provide actionable insights for proactive defense.

User and entity behavior analytics: A substantial number of cyberattacks on fintech systems emerge from insider threats. AI and ML models deployed alongside fintech infrastructure can analyze user behavior, access patterns, and contextual data to learn about user behaviors. These models can trigger alerts when they detect deviations from normal user behavior.

AI and ML limitations in fintech security
Although AI and ML offer significant cybersecurity benefits to fintechs, they are also vulnerable to various limitations that impede their efficacy and usability. Some of these issues raise ethical and legal concerns that limit the exploitation of the technologies in security. They include;

Data privacy concerns
Artificial intelligence and machine learning models are trained using data. While most of this data is simulated and collected from digital sources, some training requires actual data from people. Using real customer data in model training is subject to privacy concerns. Misuse of customer data may attract ethical and legal ramifications.

Adversarial attacks
Although AI and ML models effectively detect and mitigate cyberattacks, modern attackers are finding strategies and loopholes to bypass these systems. Contemporary hackers are introducing carefully crafted inputs in AI and ML systems to compromise their efficacy in detecting threats.

Bias in AI systems
One of the biggest challenges of AI systems is their bias in the decision-making process. Typically, AI bias stems from bias in training data, biased algorithms, or biased data interpretation approaches. AI bias often results in false negatives or false positives. For example, AI systems may flag legitimate transactions as suspicious, preventing genuine users from using their apps.

2. Conclusion

Fintechs largely relies on digital technologies to reach customers and manage their operations. Although these platforms offer users conveniences such as ease of accessibility and cost benefits, they are vulnerable to cyber threats because of their wide attack surface and business nature. AI and ML models present a novel approach for fintechs to address the rising cyber threat in the sector. These technologies can automate security processes, hence eliminating human inefficiencies, monitoring systems 24/7,

and managing threats in real time. They can also be used in threat intelligence operations to safeguard fintech systems proactively. The use of AI and ML in fintechs' security systems not only enhances the cybersecurity status of the systems but is also cost-effective.

References

[1] Adeyoju, F. I. P. (2019). Cybercrime and cybersecurity: FinTech's greatest challenges. *Available at SSRN 3486277*.

[2] Najaf, Khakan, Md Imtiaz Mostafiz, and Rabia Najaf. "Fintech firms and banks sustainability: why cybersecurity risk matters?." *International Journal of Financial Engineering* 8.02 (2021): 2150019.

[3] Kamoun, F., Iqbal, F., Esseghir, M. A., & Baker, T. (2020, October). AI and machine learning: A mixed blessing for cybersecurity. In *2020 International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1-7). IEEE.

[4] Vantage Market Research (2023), Fintech Market – Global industry assessment and forecast. Retrieved From: https://www.vantagemarketresearch.com/industry-report/fintech-market-1543

[5] Fintech Magazine (2022), FintechsPrioritise Cybersecurity as Global Threat Increases. Retrieved From: https://fintechmagazine.com/digital-payments/fintechs-prioritise-cybersecurity-as-global-threat-increases

[6] Fugue (2020), Fugue Survey Finds Widespread Concern Over Cloud Security Risks During the COVID-19 Crisis. Retrieved From: https://www.fugue.co/press/releases/fugue-survey-finds-widespread-concern-over-cloud-security-risks-during-the-covid-19-crisis

[7] Mission Critical Magazine (2022), Fintech expert warns on rising phishing attacks. Retrieved From: https://www.missioncriticalmagazine.com/articles/94237-fintech-expert-warns-on-rising-phishing-attacks